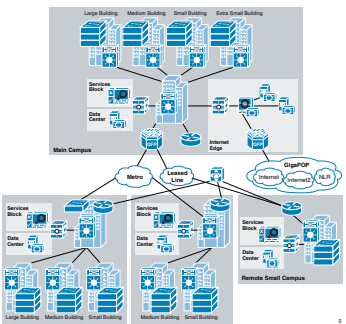
WAN Design

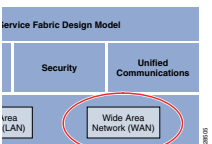
The Cisco Community College reference design is a multi-campus design where a campus consists of multiple buildings and services. The campuses are interconnected through various WAN transports as shown in Figure 1.

Figure 1 Community College WAN Design Diagram



Within the Community College reference design, the service fabric network provides the foundation on which all the solutions and services are built upon to solve the business challenges facing community colleges. These challenges include virtual learning, secure connected classrooms, and safety and security. This service fabric consists of four distinct components as shown in Figure 2.

Figure 2 The Service Fabric Design Model



This chapter discusses the WAN design component of the community college service fabric design. This section discusses how the WAN design is planned for community colleges, the assumptions made, the platforms chosen, and the justification for choosing a platform. The WAN design is highly critical to provide network access for remote campus locations to the main campus site, as well as connectivity between community colleges, and general Internet access for the entire college. The WAN design should not be viewed merely for providing access, but mainly to see how the business requirements can be met. In today's collaborative learning environment, it is important for communication to exist between students and teachers. This communication could be with voice, video, or data applications. Moreover, the video applications, may possess, flavors ranging from desktop video to real-time video. To provide this collaborative environment, highly resilient and, highly performing, WAN designs are required.

The main components of Community College WAN design are as follows:

- WAN transport
- WAN devices
- Network Foundation services—Routing, QoS, and multicast

WAN Transport

This section discusses the different WAN transports present in the community college.

Private WAN Service

One of the main requirements for community colleges is the ability to collaborate with other colleges within North America and globally. To achieve the inter connectivity between the colleges, the network should be connected to certain providers, such as Lambda rail, Internet2. The community colleges need to connect to Gigapops—regional networks, which provide access to these private WAN networks. The following sections provide a brief description on these two network types:

Internet2 is a not-for-profit advanced networking consortium comprising more than 200 U.S. universities in cooperation with 70 leading corporations, 45 government agencies, laboratories, and other institutions of higher learning as well over 50 international partner organizations. Internet2 provides its members both leading-edge network capabilities and unique partnership opportunities that together facilitate the development, deployment and use of revolutionary Internet technologies. The Internet2 network's physical implementation is comprised of an advanced IP network, virtual circuit network and core optical network. It provides the necessary scalability for member institutions to efficiently provision resources to address bandwidth-intensive requirements of their campuses such as, collaborative applications, distributed research experiments, grid-based data analysis and social networking. For more information on the Internet2 network, refer to the following URL:

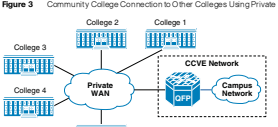
http://www.internet2.edu/network/

National LambdaRail (NLR) is a high-speed, fiber-optic network infrastructure linking over 30 cities in 21 states. It is owned by the U.S. research and education community and is dedicated to serving the needs of researchers and research groups. NLR's high-performance network backbone offers unrestricted usage and bandwidth, a choice of cutting-edge network services and applications, and customized service for individual researchers and projects. NLR services include high-capacity 10Gb Ethernet LAN-PHY or OC-192 lambdas, point-to-point or multipoint Ethernet-based transport, routed IP-based services, and TelePresence video-conference services. For more information on the NLR network and its services, refer to the following URL:

http://www.nlr.net/

This design assumes that community colleges are connected to one of these networks using either Layer 2 or Layer 3 networks for WAN connectivity, using WAN speeds of 100Mbs. The physical connection is assumed to be one connection to the service provider, but there will be two logical connections—one for accessing private networks, and the second one for Internet access. Figure 3 depicts how community college would connect to different colleges, universities, and research networks using either NLR or Internet2 service.

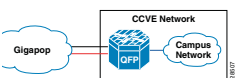
Figure 3 Community College Connection to Other Colleges Using Private WAN



Internet Service

The physical connection for reaching the Internet and the private WAN network is same; however, both circuits are logically separated using different sub-interfaces. Therefore, it is similar to a situation where a customer is connected to different service providers. See Figure 4.

Figure 4 Community College Internet Service



Metro Service

Metro Ethernet is one of the fastest growing WAN transport technologies in the telecommunications industry. The advantages of using this WAN transport are as follows:

- Scalability and reachability
  - The services offered would scale from 1Mbps to 10Gbps, and beyond in granular increments, which makes this transport highly scalable.
  - Service providers worldwide are migrating their networks to provide metro services; thereby, it is available at large number of places.
- Performance, QoS, and suitability for convergence
  - Inherently Ethernet networks require less processing to operate and manage and operate at higher bandwidth than other technologies.
  - The granular options in bandwidth, ability to provide different SLA based on voice, video, and data applications that provide QoS service to customers.
  - Low latency and delay variation make it the best solution for video, voice, and data.
- Cost savings
  - Metro Ethernet brings the cost model of Ethernet to the WAN.
- Expediting and enabling new applications
  - Accelerates implementations with reduced resources for overburdened IT departments.
  - Enables new applications requiring high bandwidth, and low latency that were previously not possible or prohibited by high cost.

There are two popular methods of service for Metro Ethernet:

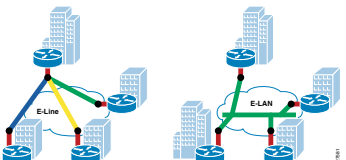
1. E-line, which is also known as Ethernet Virtual Private Line (EVPL) provides a point-to-point service.
2. E-LAN which provides multipoint or any-to-any connectivity.

EVPL, like Frame Relay, provides for multiplexing multiple point-to-point connections over a single physical link. In the case of Frame Relay, the access link is a serial interface to a Frame Relay switch with individual data-link connection identifiers (DLCIs), identifying the multiple virtual circuits or connections. In the case of EVPL, the physical link is Ethernet, typically FastEthernet or Gigabit Ethernet, and the multiple circuits are identified as VLANs by way of an 802.1q trunk.

E-LAN, also known as Virtual Private LAN Services (VPLS), provides any-to-any connectivity within the Metro area, which allows flexibility. It passes 802.q trunks across the SP network known as Q-in-Q.

Figure 5 shows the difference between these services.

Figure 5 Different Services Available

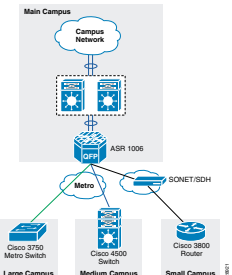


This section discusses how the Metro service is designed in the Community College reference design. The Metro service is used to provide connectivity between the remote campuses to the main campus site. The key reasons for recommending Metro service for community college are as follows:

- *Centralized administration and management*—E-line service provides point-to-point connectivity, where as, E-LAN provides point-to-multipoint connectivity. Having a point-to-point connectivity mandates that all the remote campus sites need to traverse the main campus site to reach the other, making the centralized administration applicable.
- *Performance*—Since all the application services are centrally located at main campus site, the WAN bandwidth required for remote campus sites to main campus site should be at least 100 Mbps. The Metro transport can provide 100Mbps, and more if needed in the future.

Therefore, in this design, it is recommended that the remote large and remote medium campus locations use E-line service to connect to the main campus site. Figure6 shows how the remote campus locations are connected to main campus site using Metro service.

Figure 6 The Metro Transport Deployment in Community College WAN Design



Leased-Line Service

The WAN bandwidth requirement for a small remote site is assumed to be 20Mbps. Cisco recommends that the remote small campus site connect to the main campus site using a private leased-line service. The leased-line service is more readily available for these type of locations and the bandwidth is sufficient for the remote small campus application requirements.

WAN Aggregation Platform Selection in the Community College Reference Design

In addition to selecting the WAN service for connectivity between college campus locations and access to the Internet, choosing the appropriate WAN aggregation router is essential. For each location in the Community College reference design, various WAN aggregation platforms are selected based on the requirements.

Main Campus WAN Aggregation Platform Selection

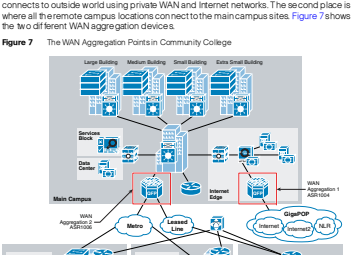
A WAN aggregation router aggregates all the incoming WAN circuits from various locations in the network as well as the Internet and also provides the proper QoS required for application delivery. Cisco recommends the Cisco ASR family of routers as the WAN aggregation platform for the main campus location.

The Cisco ASR 1000 Series Router family consists of three different models:

- The Cisco ASR 1002 Router is a 3-SPA, 2-rack-unit (RU) chassis with one Embedded Services Processor (ESP) slot that comes with an integrated Router Processor (RP), integrated Cisco ASR 1000 Series Shared Port Adapter Interface Processor (SIP), and integrated four Gigabit Ethernet ports.
- The Cisco ASR 1004 Router is an 8-SPA, 4-RU chassis with one ESP slot, one RP slot, and two SIP slots.
- The Cisco ASR 1006 Router is a 12-SPA, 6-RU, hardware redundant chassis with two ESP slots, two RP slots and three SIP slots.

In community college WAN design, there are two places where the WAN aggregation occurs in the main campus location. The first place is where the main campus location connects to outside world using private WAN and Internet networks. The second place is where all the remote campus locations connect to the main campus sites. Figure 7 shows the two different WAN aggregation devices.

Figure 7 The WAN Aggregation Platforms in Community College



WAN Aggregation 1

Cisco ASR 1004 Series router is recommended as WAN aggregation platform for private WAN/Internet connectivity. This choice was made considering the cost and required features—performance, QoS, routing, and resiliency, which are essential requirements for WAN aggregation router. Moreover, this platform contains built-in resiliency capabilities such as ISSU and IOS-based redundancy.

WAN Aggregation 2

The second WAN aggregation device provides connectivity to the large and medium remote community college campuses. To perform this aggregation, the Cisco ASR 1006 router with redundant route processors and redundant ESPs has been recommended for the following reasons:

- *Performance*—Up to 20 Gbps throughput
- *Port density*—Up to 12 shared port adapters (SPAs), the highest port density solution of the three Cisco ASR 1000 routers
- *Resiliency*—Cisco ASR 1006 router supports hardware redundancy and in-service software upgrades (ISSU). This chassis would support dual route processors, and dual ESP modules to support the hardware redundancy. Moreover, this router would also support EtherChannel load balancing feature.

Remote Large Campus WAN Aggregation Platform Selection

The WAN connectivity between the large remote campus sites to the main campus site is fairly simple because of the lack of requirements of advanced encryption technologies. Therefore, the main idea is to reduce the cost and try to consolidate the WAN functionality into the distribution device at the large campus site. However, at the large campus site, as per the campus LAN design document VSS has been chosen as distribution switch, and it does not support WAN functionality. Therefore, a dedicated WAN aggregation device needed to perform that functionality, and the choice can be an ASR, 7200, or 3750ME switches. Out of these choices, considering the cost/performance criteria, the Cisco 3750ME switch was selected to perform the WAN aggregation. The Cisco 3750 Metro switch has the following features/capabilities to adequately meet the requirements:

- Hierarchical QoS
- Routing support: OSPF, EIGRP, BGP
- Multicast support: PIM
- Redundant power supply

Remote Medium Campus WAN Aggregation Platform Selection

As discussed in the *Community College LAN Deployment Guide* the remote medium campus collapses the WAN edge and core-layer LAN functionality into a single switch to provide cost effectiveness to meet the budget needs for this size location. The remote medium campus location is connected to the main campus location through Metro service. At the remote medium campus location, the WAN and LAN aggregation platform is the Cisco Catalyst 4507 switch. This switch has necessary features to perform as WAN router. However, if there is the need for advanced WAN features such as MPLS, the Cisco Catalyst 3750ME or Cisco ISR Series router or upgrading to the Cisco Catalyst 6500 series could be explored as an option. For this design, the Cisco Catalyst 4500 Series switches has been chosen to perform the dual functionality as WAN router, in addition to its role as core-layer LAN switch.

Remote Small Campus WAN Aggregation Platform Selection

The remote small campus is connected to main campus using a private leased-line service. The WAN speed between the remote small campus and the main campus location is assumed to be around 20Mbps, and this service is provided by a traditional leased line. Since it is a leased-line circuit, WAN devices such as Cisco 3750 Metro or 4507 switch can not be used. Therefore, an integrated services router is needed to meet the requirement. For this reason, the Cisco 3845 Series router is chosen as WAN platform for remote small campus. The main advantages of using the Cisco 3845 Series router are as follows:

- Enhanced Network Module Slot
- Support for over 90 existing and new modules
- Voice Features: Analog and digital voice call support and optional voice mail support
- Support for majority of existing AIMs, NMs, WICs, VWICs, and VICs
- Integrated GE ports with copper and fiber support

Implementation of Community College WAN Reference Design

The following section would discuss on the implementation details for Community College WAN Reference design. The major components of the implementation are the following:

- WAN infrastructure design
- Routing
- QoS
- Resiliency
- Multicast

WAN Infrastructure Design

As explained in the design considerations, the Community College WAN design uses two different services to connect remote campus locations to main campus location. The remote large campus site, and remote medium campus sites would connect to main campus site using Metro services. The remote small campus site uses leased-line service to connect to the main campus location. The remote large campus site, due to its size, is recommended to have 1Gbps Metro service to the main campus site where as the remote small campus location is recommended to have at least 20Mbps of bandwidth to main campus site. The following section provides the configuration details of all the WAN devices needed to establish the WAN connectivity.

Configuration of WAN interfaces at WAN Aggregation router 2

The following is configuration of WAN interfaces on WAN aggregation router 2, which aggregates all the connections from the remote campus locations to main campus site.

```
interface GigabitEthernet0/2/0
 description Connected to cr11-3750ME-RLC
 ip address 10.126.0.1 255.255.255.254
!
interface GigabitEthernet0/2/1
 description Connected to cr11-4507-RMC
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 negotiation auto
 cdp enable
 service-policy output PARENT_POLICY
 hold-queue 2000 in
 hold-queue 2000 out
!
interface GigabitEthernet0/2/1.102
 encapsulation dot1Q 102
 ip address 10.126.0.3 255.255.255.254
!
!
```

Configuration of WAN Interface at 3750 Remote Large Campus

The following is configuration of WAN interface at 3750 remote large campus switch, which is connected to main campus site:

```
interface GigabitEthernet1/1/1
 description Connected to cr11-ASR-WE
 no switchport
 dampening
 ip address 10.126.0.0 255.255.255.254
```

Configuration of WAN interface at 4500 Remote Medium Campus

The following is the configuration of WAN interface at remote medium campus connected to main campus site:

```
interface GigabitEthernet4/1
 description link connected to  cr13-6500-pe2 gi3/2
 switchport trunk native vlan 802
 switchport trunk allowed vlan 102
 switchport mode trunk
 logging event link-status
 load-interval 30
 carrier-delay msec 0
 no cdp enable
 spanning-tree portfast trunk
 spanning-tree guard root
!
interface Vlan102
 description Connected to cr11-ASR-WE
 dampening
```

```
ip address 10.126.0.2 255.255.255.254
load-interval 30
carrier-delay msec 0
```

Leased-Line Service

The WAN bandwidth requirement for a small remote site is assumed to be 20Mbps. Cisco recommends that the remote small campus site connect to the main campus site using a private leased-line service. The leased-line service is more readily available for these type of locations and the bandwidth is sufficient for the remote small campus application requirements. To implement this design, a serial SPA is needed on the ASR 1006 WAN aggregation router at the main campus site and this SPA needs to be enabled for T3 interface type. The following configuration illustrates how to enable and configure the T3 interface:

The following configuration steps are needed to build the lease-line service between the main campus and remote small campus:

1. Enable the T3 interface on the SPA on ASR1006

```
card type t3 0 3
```

2. Configure the WAN interface

```
interface Serial0/3/0
 dampening
 ip address 10.126.0.5 255.255.255.254
```

Configuration of WAN Interface at Remote Small Campus Location

The following is configuration of WAN interface at remote small campus location:

```
interface Serial2/0
 dampening
 ip address 10.126.0.4 255.255.255.254
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp-key
 ip pim sparse-mode
 service-policy output RSC_PARENT_POLICY
 ip summary-address eigrp 100 10.124.0.0 255.255.0.0 5
 load-interval 30
 carrier-delay msec 0
 dsu bandwidth 44210
```

Routing Design

This section discusses how routing is designed and implemented in the Community College reference WAN design. As indicated in the WAN transport design, the Community College reference design has multiple transports—NLR or I2 networks, Internet, Metro Service, and leased-line services. The NLR or I2 networks would provide access to reach other community colleges, universities, and research networks globally. Internet service would help the Community College to reach Internet. Metro/leased-line service would help to connect remote campus locations to the main campus. To provide connectivity using these transport services we have designed two distinct routing domains – external and internal. The external routing domain is where the Community College would connect with external autonomous system, and the internal routing domain is where the entire routing domain is within single autonomous system. The following section would discuss about the external routing domain design, and the internal routing domain design.

External Routing Domain

As indicated above, the external routing domain would connect with different service providers, NLR or I2, and the Internet service. This is applicable only to the WAN aggregation router 1, which interfaces with both NLR or I2, and the Internet service, because it the only router which interfaces with the external domain.

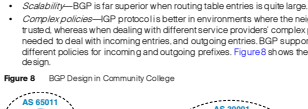
The main design considerations for routing for the Internet/private WAN edge router are as follows:

- Scale up to large number of routes
- Support for multi-homing—connection to different service providers
- Ability to implement complex polices—Have separate policies for incoming and outgoing traffic

To meet the above requirements, BGP has been chosen as the routing protocol because of the following reasons:

- *Scalability*—BGP is far superior when routing table entries is quite large.
- *Complex policies*—IGP protocol is better in environments where the neighbors are trusted, whereas when dealing with different service providers' complex policies are needed to deal with incoming entries, and outgoing entries. BGP supports having different policies for incoming and outgoing prefixes. Figure 8 shows the BGP design.

Figure 8 BGP Design in Community College



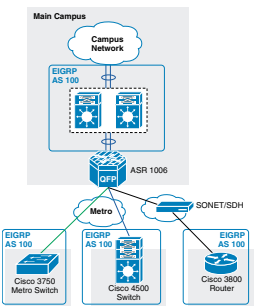
For more information on designing and configuring BGP on the Internet border router, refer to the *SAFE Reference Design* at the following link:

http://www.cisco.com/en/US/netsol/ns954/index.html#~five

Internal Routing Domain

EIGRP is chosen as the routing protocol for designing the internal routing domain, which is basically connecting all the devices in the campus network. EIGRP is a balanced hybrid routing protocol that builds neighbor adjacency and flat routing topology on per autonomous-system (AS)-basis. It is important to design EIGRP routing domain in college infrastructure with all the design principles defined earlier in this section. CCVE SRA network infrastructure must be deployed in recommended EIGRP protocol design to secure, simplify, and optimize the network performance. Figure 9 depicts the design of EIGRP for internal network.

Figure 9 EIGRP Design Diagram



EIGRP Configuration on WAN Aggregation Router 2 –ASR1006

The EIGRP is used on the following links:

1. Port-channel link, which is link between the ASR1006 router and the core.
2. The 1Gbps Metro link to remote large campus location.
3. The 100Mpbs Metro link to remote medium campus location.
4. 20Mbps leased-line service to remote small campus location.

The configurations steps are as follows:

1. Configure the neighbor authentication on interface links:

```
interface Port-channel1
 ip address 10.125.0.23 255.255.255.254
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp-key
!
interface GigabitEthernet0/2/0
 description Connected to cr11-3750ME-RLC
 ip address 10.126.0.1 255.255.255.254
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp-key
!
interface GigabitEthernet0/2/1
 description Connected to cr11-4507-RMC
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 negotiation auto
 cdp enable
 hold-queue 2000 in
 hold-queue 2000 out
!
interface GigabitEthernet0/2/1.102
 encapsulation dot1Q 102
 ip address 10.126.0.3 255.255.255.254
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp-key
!
interface Serial0/3/0
 dampening
 ip address 10.126.0.5 255.255.255.254
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp-key
```

2. Configure the summarization on the member links:

```
interface Port-channel1
 ip address 10.125.0.23 255.255.255.254
 ip summary-address eigrp 100 10.126.0.0 255.255.0.0 5
!
interface GigabitEthernet0/2/0
 description Connected to cr11-3750ME-RLC
 ip address 10.126.0.1 255.255.255.254
 ip summary-address eigrp 100 10.126.0.0 255.255.0.0 5
```

```
!
interface GigabitEthernet0/2/1
 description Connected to cr11-4507-RMC
!
interface GigabitEthernet0/2/1.102
 encapsulation dot1Q 102
 ip address 10.126.0.3 255.255.255.254
 ip summary-address eigrp 100 10.126.0.0 255.255.0.0 5
!
interface Serial0/3/0
 ip address 10.126.0.5 255.255.255.254
 ip summary-address eigrp 100 10.126.0.0 255.255.0.0 5
```

3. Configure EIGRP routing process:

```
router eigrp 100
 network 10.0.0.0
 eigrp router-id 10.125.200.24
 no auto-summary
 passive-interface default
 no passive-interface GigabitEthernet0/2/0
 no passive-interface GigabitEthernet0/2/1.102
 no passive-interface Serial0/3/0
 no passive-interface Port-channel1
 nsf
```

The ASR1006 router is enabled with non-stop forwarding feature. The following command is used to verify the status:

```
cr11-asr-we#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
  EIGRP NSF-aware route hold timer is 240s
  EIGRP NSF enabled
      NSF signal timer is 20s
      NSF converge timer is 120s
      Time since last restart is 2w1d
  Automatic network summarization is not in effect
  Address Summarization:
    10.126.0.0/16 for Port-channel1, GigabitEthernet0/2/0,
GigabitEthernet0/2/1.102
      Serial0/3/0
      Summarizing with metric 2816
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
  Passive Interface(s):
    GigabitEthernet0/2/1
    GigabitEthernet0/2/2
    GigabitEthernet0/2/3
    GigabitEthernet0/2/4
    Serial0/3/1
    Group-Async0
    Loopback0
    Tunnel0
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)         90      2w1d
    10.125.0.22           90      1d17h
    10.126.0.4            90      1d17h
    10.126.0.0            90      1d17h
    10.126.0.2            90      1d17h
  Distance: internal 90 external 170


cr11-asr-we#
```

EIGRP Configuration on 3750 Remote Large Campus Switch

The EIGRP configuration at 3750 remote large campus site also has similar steps compared to Main campus site.

4. Enable authentication on the link:

```
interface GigabitEthernet1/1/1
 description Connected to cr11-ASR-WE
 no switchport
 dampening
 ip address 10.126.0.0 255.255.255.254
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp-key
 router eigrp 100
 network 10.0.0.0
 passive-interface default
 no passive-interface Port-channel1
 no passive-interface GigabitEthernet1/1/1
 eigrp router-id 10.122.200.1
```

5. Configure summarization on the link:

```
interface GigabitEthernet1/1/1
 description Connected to cr11-ASR-WE
 no switchport
 dampening
 ip address 10.126.0.0 255.255.255.254
 ip summary-address eigrp 100 10.122.0.0 255.255.0.0
```

6. Configure EIGRP routing process:

```
router eigrp 100
 network 10.0.0.0
 passive-interface default
 no passive-interface Port-channel1
 no passive-interface GigabitEthernet1/1/1
 eigrp router-id 10.122.200.1
!
```

EIGRP Configuration at 4750 Medium Campus Switch

7. Enable authentication on the WAN link:

```
interface Vlan102
 description Connected to cr11-ASR-WE
 dampening
 ip address 10.126.0.2 255.255.255.254
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp-key
Step2) Enable summarization on the WAN links
interface Vlan102
 ip summary-address eigrp 100 10.123.0.0 255.255.0.0 5
 load-interval 30
 carrier-delay msec 0
```

8. Enable EIGRP routing process:

```
router eigrp 100
 passive-interface default
 no passive-interface Vlan102
 no auto-summary
 eigrp router-id 10.123.200.1
 network 10.98.0.1 0.0.0.0
 network 10.123.0.0 0.0.255.255
 network 10.126.0.0 0.0.255.255
 nsf
!
```

EIGRP Configuration at 3800 Remote Small Campus Router

9. Configure link authentication:

```
interface Serial2/0
 dampening
 ip address 10.126.0.4 255.255.255.254
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp-key
```

10. Step2) Configure Summarization

```
 interface Serial2/0
 dampening
 ip summary-address eigrp 100 10.124.0.0 255.255.0.0 5
 load-interval 30
 carrier-delay msec 0
 dsu bandwidth 44210
```

11. Configure EIGRP process:

```
router eigrp 100
 network 10.0.0.0
 no auto-summary
 eigrp router-id 10.124.200.1
!
```

To obtain more information about EIGRP design, refer to the *Community College LAN Deployment Guide*.

QoS

QoS is a part of foundation services, which is very critical to the application performance. Today's networks are rapidly converging into IP network. The traditional applications, which used the networks, were voice, video, and data. However, broadcast video, real-time video, video surveillance, and many other applications have all converged into IP networks. Moreover, each of these applications require different performance characteristics on the network. For example, data applications may need only high throughput, but are tolerant to delay and loss. Similarly, voice applications need constant low bandwidth and low delay performance. To cater to these performance characteristics, Cisco IOS has several rich QoS tools such as classification and marking, queuing, WRED, policing, shaping, and many other tools to effect the traffic characteristics. Before discussing the QoS design, the following subsection provides a brief introduction on these characteristics.

Traffic Characteristics

The main traffic characteristics are bandwidth, delay, loss, and jitter.

- *Bandwidth*—Lack of proper bandwidth can cause applications from performing poorly. This problem would be exacerbated if there were more centralized applications. The bandwidth constraint occurs because of the difference between the bandwidth available at LAN and the WAN. As shown in Figure 10, the bandwidth of the WAN transport dictates the amount of traffic received at each remote site. Applications are constrained by the amount of WAN bandwidth.

Figure 10 Bandwidth Constraint Due to Difference in Speeds

- *Jitter*—Occurs when there are bandwidth mismatches between the sender and receiver, which could result in poor performance of delay sensitive applications like voice and video.
- *Loss*—occurs when the queues become full, and there is not enough bandwidth to send the packets.
- *Delay*—Is an important characteristic, which plays a large role in determining the performance of the applications. For a properly designed voice network the one-way delay must be less then 150 msec.

QoS Design for WAN Devices

For any application regardless of whether it is video, voice, or data the traffic characteristics just mentioned need to be fully understood before making any decisions on WAN transport or the platforms needed to deploy these services. Cisco QoS tools help to optimize these characteristics so that voice, video, and data applications performance is optimized. The voice and video applications are highly delay-and drop-sensitive, but the difference lies in the bandwidth requirement. The voice applications have a constant and low bandwidth requirement, but the video applications have variable bandwidth requirements. Therefore, it is important to have a good QoS policy to accommodate these applications.

Regardless of the WAN transport chosen, QoS design is the most significant factor in determining the success of network deployment. There are number of benefits in deploying a consistent, coherent QoS scheme across all network layers. It helps not only in optimizing the network performance, it helps to mitigate network attacks, and also manage the control plane traffic. Therefore, when the platforms are selected at each network layer, QoS must always be considered in the design choice.

In the WAN links the congestion can occur when there are speed mismatches. This may occur because there is significant difference between LAN speeds and WAN speeds. To prevent that from occurring, the following two major tools can be used:

- Low-Latency Queuing (LLQ), which is used for highest-priority traffic (voice/ video).
- Class-based Weighted-Fair Queuing (CBWFQ), which can be used for guaranteeing bandwidth to data applications.

The general guidelines for deploying the WAN edge device considerations are as follows:

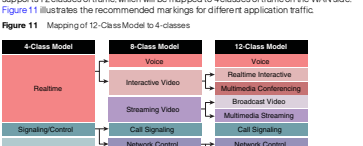
- For WAN speeds between 1Mpbs to 100Mbps, use hierarchical policies for sub-line-rate Ethernet connections to provide shaping and CBWFQ/LLQ.
- For WAN speeds between 100Mbps to 10Gbps, use ASR1000 with QFP or hardware queuing via Cisco Catalyst 3750-Metro and 6500/7600 WAN modules.

When designing the QoS for WAN architecture, there are two main considerations to start with:

- Whether the service provider will provide four classes of traffic.
- The service provider will only provide one class of traffic.

This document assumes that the service provider will support at least 4 classes of traffic such as REAL_TIME, GOLD, SILVER, and DEFAULT. The community college campus LAN supports 12 classes of traffic, which will be mapped to 4 classes of traffic on the WAN side. Figure 11 illustrates the recommended markings for different application traffic.

Figure 11 Mapping of 12-Class Model to 4-classes



Once the QoS policy is designed the next pertinent question is the appropriate allocation of bandwidth for the 4 classes of traffic. Table 1 describes the different classes, and the percentage, and actual bandwidth allocated for each class of traffic.

Table 1 QoS Classes

Class of Traffic	4-class SP Model	Bandwidth Allocated	Actual Bandwidth
Voice, Broadcast Video, RealTime Interactive	SP- Real-Time	30%	33 Mbps
Network Control Signaling Transactional Data	SP-Critical 1	20%	36 Mbps
Multi-media Conferencing Multimedia streaming OAM	SP-Critical 2	20%	25 Mbps
Bulk data Scavenger Best Effort	SP-Best Effort	30%	6 Mbps

QoS Implementation

This section discusses how QoS is implemented in community college WAN design network. As explained in the QoS design considerations, the main objective of the QoS implementation is to ensure that the 12 classes of LAN traffic is mapped into 4 classes of WAN traffic. Each class should receive the adequate bandwidth, and during congestion, each class must received the guaranteed minimum bandwidth. To accomplish this objective, the following methods are used to implement QoS policy:

- *Three-layer hierarchical design*—This is needed when multiple sites need to share a common bandwidth, and each site needs dedicated bandwidth, and queuing within the reserved policy.
- *Two-layer hierarchical design*—This design is needed when the interface bandwidth is higher than the SLA bandwidth allocated by the service provider. For example, if the physical link is 100Mbs, but the service provider has only allocated 50 Mbps. In this scenario we need two policies. The first policy, which is parent policy would shape the entire traffic to 50Mbs then the child policy would queue and allocated bandwidth for each class.
- *Single-layer design*—If the interface bandwidth, and the SLA bandwidth of the provider are equal then we can use a single QoS policy to share the bandwidth among the classes of traffic, which is four in our design.

This section describes detailed implementation of QoS policies at various parts of the network. The devices that need QoS design are as follows:

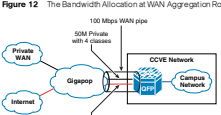
- WAN aggregation router 1 for connection to the Internet and NLR network
- WAN aggregation router 2 for connection to remote campus sites
- Cisco 3750 Metro switch at the remote large campus
- Cisco 4500 switch at the remote medium campus
- Cisco 3800 router at the remote small campus

QoS Implementation at WAN Aggregation Router 1

The WAN aggregation router1 connects to two different providers: NLR network and Internet. It is assumed that the aggregate bandwidth is 100Mbps that should be shared between both services—50Mbps is dedicated for NLR network and 50Mbps is dedicated for Internet traffic. As explained in the previous section, to implement this granular policy, a three-layer hierarchical QoS design needs to be implemented.

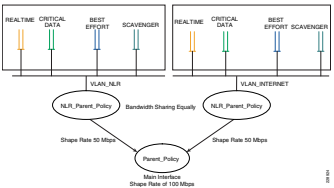
Figure12 depicts the bandwidth allocation at the WAN aggregation router 1.

Figure 12 The Bandwidth Allocation at WAN Aggregation Router 1



To implement a three-layer hierarchical QoS policy on the WAN aggregation1 router, a higher-level parent policy is defined that would shape the aggregate WAN speed to 100Mbps, then sub-parent policies are defined, which would further shape it to 50Mbps. Within each of the sub-parent policies, there are four defined classes: REALTIME, CRITICAL_DATA, BEST_EFFORT, and SCAVENGER classes. Figure13 depicts this hierarchical QoS design.

Figure 13 Hierarchical QoS Design



The hierarchical three-layer QoS policy is implemented in three steps as follows:

1. Define Parent policy—Enforces the aggregate bandwidth policy for the entire interface. This is like a Grandfather of policy.
2. Define the individual sub-parent policies—These would be specific to each service type. For example, NLR_PARENT is a policy dedicated for NLR traffic, and NLR_Internet is specific to Internet traffic.
3. Define the child policies—Classifies, queues, and allocate bandwidth within each sub-parent policy. For example, NLR_PARENT would have a NLR_Child policy that would classify, queue, and allocate the bandwidth within each allocated bandwidth. The following diagram shows the hierarchical allocation.

Implementation Steps for Qos Policy at WAN Aggregation Router 1

This section would describes the detailed steps needed to implement the three-layer QoS policy in the WAN_Aggregation_router1.

1. Define class-maps.

```
class-map match-all REALTIME
 match ip dscp cs4  af41  cs5  ef

class-map match-all CRITICAL_DATA
 match ip dscp af11  af21  cs3  cs6

class-map match-all BEST_EFFORT
 match ip dscp default

class-map match-all SCAVENGER
 match ip dscp cs2
```

239835

1. Define child policy maps.

```
policy-map IE_CHILD_POLICY
 class REALTIME
  priority percent 33
 class CRITICAL_DATA
  bandwidth remaining ratio 6
 class SCAVENGER
  bandwidth remaining ratio 1
 class BEST_EFFORT
  bandwidth remaining ratio 4

policy-map NLR_CHILD_POLICY
 class REALTIME
  priority percent 33
 class CRITICAL_DATA
  bandwidth remaining ratio 6
 class BEST_EFFORT
  bandwidth remaining ratio 4
 class SCAVENGER
  bandwidth remaining ratio 1
```

239837

2. Define parent policy maps.

```
class-map match-all dummy                          ← Dummy class does not classify anything
!
policy-map PARENT_POLICY
 class dummy service-fragment share                ← Defining service-fragment would allow other
  shape average 10000000                             policies to point for share of bandwidth.
                                                   ← The parent policy would shape to 100 Mbps.
policy-map NLR_PARENT_POLICY
 class class-default fragment share
  shape average 50000000                           ← Parent policy allocates 50% of bandwidth
  service-policy NLR_CHILD_POLICY                  ← Child policy gets attached to parent policy
!
policy-map IE_PARENT_POLICY
 class class-default fragment share
  shape average 50000000
  service-policy IE_CHILD_POLICY
!
```

239838

3. Apply the policy maps created in Steps 1 to 3.

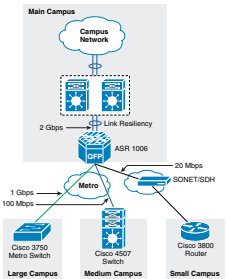
```
interface GigabitEthernet1/0/0
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 negotiation auto
 service-policy output PARENT_POLICY              ← Aggregate policy (grand-father) applied on
 hold-queue 2000 in                                 main interface
 hold-queue 2000 out
!
interface GigabitEthernet1/0/0.65
 description link to 6500
 encapsulation dot 1Q.65
 ip address 64.104.10.113 255.255.255.252
 service-policy output IE_PARENT_POLICY           ← The parent policy applied on sub-interface
!
interface GigabitEthernet1/0/0.75
 description link to 6500
 encapsulation dot 1Q.75
 ip address 64.104.10.125 255.255.255.252
 service-policy output NLR_PARENT_POLICY
!
```

239839

QoS Policy Implementation for WAN Aggregation Router 2

QoS configuration at WAN aggregation router 2 is more complex than the QoS configuration of WAN aggregation router 1 because of different speeds connected to the router. Figure 14 depicts the different types of WAN speeds.

Figure 14 WAN Link Speeds at WAN Aggregation Router 2 Device



The requirements of the QoS design at the WAN aggregation router 2 are as follows:

- The link speed between the main campus, and large campus is 1Gbps. Therefore, a single-layer QoS policy can be defined on the link.
- The SLA between the main campus, and medium campus is assumed to be 100Mbps; however, link speed is assumed to be 1Gbps. In addition, there is an assumption that there could be more than one medium campus present in this design. Therefore, each remote medium campus would connect to the main campus using these 100Mbps links, requiring a three-layer hierarchical QoS policy is needed.The link between the main campus and remote small campus is 20Mbps. The physical link speed is 44Mbps, requiring a two-level hierarchical QoS policy is needed.
- The Ether channel link between the ASR router and the core is 2Gbps, which contains two links of 1Gbps link speeds. Since the physical link speed and the actual WAN speed is 1Gbps, a single-level QoS policy can be applied on each of the links.

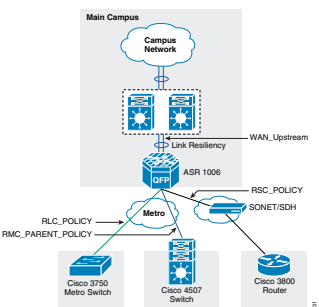
Table 2 describes the different QoS policy names applied at the WAN aggregation router 2.

Table 2 QoS Policy for WAN Aggregation Route 2

Qos Policy Name	Description	WAN Speed
RLC_POLICY	Applied on link between main campus, and remote large campus	1Gbps
PARENT_POLICY RMC_PARENT_POLICY RMC_CHILD_POLICY	Hierarchical Qos Policy between the main campus, and remote medium campus location.	100 Mbps
WAN_Upstream	Applied on link between main campus, and core	2Gbps
RSC_PARENT_POLICY RSC_POLICY	Applied on link between main campus and small campus	20Mbps

Figure 15 depicts the various points where QoS policies are applied.

Figure 15 The allocation of QoS Policy at Different Places on WAN Aggregation Router 2



QoS Policy Between the Main Campus and Large Campus

The WAN physical link speed is 1Gbs. Also, the actual SLA between the main campus and large campus is assumed to be 1Gbps. Therefore, a single-layer QoS policy is implemented in this scenario.

1. Define the class-maps.

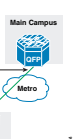
```
class-map match-all REALTIME
 match ip dscp cs4  af41  cs5  ef
class-map match-all CRITICAL_DATA
 match ip dscp af11  af21  cs3  af31 cs6
class-map match-all BEST_EFFORT
 match ip dscp default
class-map match-all SCAVENGER
 match ip dscp cs2
!
```

2. Define the policy map.

```
policy-map RLC_POLICY
 class REALTIME
  priority percent 33
  set cos 5
 class CRITICAL_DATA
  bandwidth remaining ratio 6
  set cos 3
 class SCAVENGER
  bandwidth remaining ratio 1
  set cos 0
 class BEST_EFFORT
  bandwidth remaining ratio 4
  set cos 2
!
```

3. Apply the class-maps and policy map defined in Steps 1 and 2 on the interface connected between main campus to the large campus site.

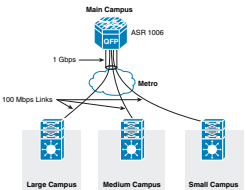
```
interface GigabitEthernet0/2/0
 description Connected to cr11-3750ME-RLC
 ip address 10.126.0.1 255.255.255.254
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp-key
 ip pim sparse-mode
 ip summary-address eigrp 100 10.126.0.0 255.255.0.0.5
 logging event link-status
 load-interval 30
 negotiation auto
 service-policy output RLC_POLICY
!
```



QoS Policy Between the Main Campus and Medium Campus Location

A three-layer QoS design is needed between the main campus site and large medium campus location because there could be couple of medium campus locations connected on a single metro link to the main campus site. Figure16 shows how this design looks like when there are more than one medium campus site.

Figure 16 The WAN Link Design for Connectivity Between Main Campus and Remote Medium Campus



Here, the implementation details are provided for only a single medium campus location; however, more medium campus locations could be added, if desired. The following are implementation steps for this QoS policy:

1. Define the child policy maps.

```
policy-map RMC_CHILD_POLICY
 class REALTIME
  priority percent 33
  set cos 5
 class CRITICAL_DATA
  bandwidth remaining ratio 6
  set cos 3
 class SCAVENGER
  bandwidth remaining ratio 1
  set cos 0
 class BEST_EFFORT
  set cos 2
```

235836

2. Define the parent policy maps.

```
class-map match-all dummy
!
policy-map PARENT_POLICY
 class dummy service-fragment share
  shape average 10000000
```
Sets the total bandwidth to 1G

```
policy-map RMC_PARENT_POLICY
 class class-default fragment share
  shape average 10000000
  service-policy RMC_CHILD_POLICY
```
Sets the bandwidth for single medium campus to 100Mbps

239837

3. Apply the policy maps.

```
interface GigabitEthernet0/2/1
description Connected to cr11-4507-RMC
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 negotiation auto
 cdp enable
 service-policy output PARENT_POLICY
 hold-queue 2000 in
 hold-queue 2000 out
!
interface GigabitEthernet0/2/1.102
 encapsulation dot1Q 102
 ip address 10.126.0.3 255.255.255.254
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp-key
 ip pim sparse-mode
 ip summary-address eigrp 100 10.126.0.0 255.255.0.0 5
 service-policy output RMC_PARENT_POLICY
```
First level policy applied to main interface

Second level policy applied to sub-interface


```
policy-map RMC_PARENT_POLICY
  class class-default fragment share
    shape average 10000000
    service-policy RMC_CHILD_POLICY
```
Third level policy applied to main parent policy

354108

QoS Policy Between Main Campus and Remote Small Campus Location

The following is the QoS policy implementation steps between main campus and remote small campus location. The actual WAN speed is 44Mbps; however, the SLA is assumed to be 20Mbps. Therefore, a two-layer hierarchical QoS design is needed to implement the above policy.

1. Define the policy map.

```
policy-map RSC_POLICY
 class REALTIME
  priority percent 33
 class CRITICAL_DATA
  bandwidth remaining ratio 6
 class SCAVENGER
  bandwidth remaining ratio 1
 class BEST_EFFORT
  bandwidth remaining ratio 4
!
```
This is child policy

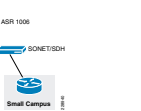
```
policy-map RSC_PARENT_POLICY
 class class-default
  shape average 20000000
  service-policy RSC_POLICY
```
This is parent policy

239839

2. Apply the policy map to the interface.

```
interface Serial0/3/0
 dampening
 ip address 10.126.0.5 255.255.255.254
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp-key
 ip pim sparse-mode
 ip summary-address eigrp 100 10.126.0.0 255.255.0.0 5
 logging event link-status
 load-interval 30
 carrier-delay msec 0
 dsu bandwidth 44210
 framing c-bit
 cablelength 10
 service-policy output RSC_PARENT_POLICY
end

cr11-asr-we#
```
Apply parent policy to interface



239840

QoS Policy Implementation Between the Main Campus and Core

The following is the QoS policy implementation between main campus and core. There are two links between the ASR 1006 and core, which is VSS. QoS policy needs to be configured on both links.

3. Define of policy-map.

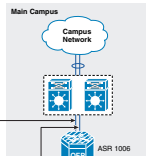
```
policy-map WAN_Upstream
 class REALTIME
  priority percent 33
 class CRITICAL_DATA
  bandwidth remaining ratio 6
 class SCAVENGER
  bandwidth remaining ratio 1
 class BEST_EFFORT
  bandwidth remaining ratio 4
```

239841

4. Apply the policy-map on both interfaces going up to the core.

```
policy-map WAN_Upstream
 class REALTIME
   priority percent 33
 class CRITICAL_DATA
   bandwidth remaining ratio 6
 class SCAVENGER
   bandwidth remaining ratio 1
 class BEST_EFFORT
   bandwidth remaining ratio 4

interface GigabitEthernet0/2/3
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 negotiation auto
 cdp enable
 service-policy output WAN_Upstream
 channel-group 1 mode active
 hold-queue 2000 in
 hold-queue 2000 out
!
interface GigabitEthernet0/2/4
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 negotiation auto
 cdp enable
 service-policy output WAN_Upstream
 channel-group 1 mode active
 hold-queue 2000 in
 hold-queue 2000 out
```



237642

QoS Policy Between Large Campus and Main Campus Location

The WAN interface between the large campus and main campus site is 1 Gbps, which is also equal to the link speed; therefore, a single-layer QoS policy map can be created.

1. Define the class-maps.

```
class-map match-all REALTIME
 match ip dscp cs4  af41  cs5  ef
class-map match-all CRITICAL_DATA
 match ip dscp af11 cs2  af21  cs3  af31 cs6
class-map match-all BEST_EFFORT
 match ip dscp default
class-map match-all SCAVENGER
 match ip dscp cs1
```

239643

2. Define the policy-map.

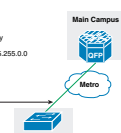
```
policy-map ME_POLICY
 class REALTIME
   priority
   police 220000000 8000 exceed-action drop
   set cos 5
 class CRITICAL_DATA
   bandwidth remaining ratio 40
   set cos 3
 class BEST_EFFORT
   bandwidth remaining ratio 35
   set cos 2
 class SCAVENGER
   bandwidth remaining ratio 25
   set cos 0
!
!
```

The realtime traffic get 330 Mbps

239644

3. Apply the QoS policy-map to the WAN interface.

```
interface GigabitEthernet1/1/1
 description Connected to cr11-ASR-WE
 no switchport
 dampening
 ip address 10.126.0.0 255.255.255.254
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp-key
 ip pim sparse-mode
 ip summary-address eigrp 100 10.122.0.0 255.255.0.0
 load-interval 30
 carrier-delay msec 0
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 service-policy output ME_POLICY
 hold-queue 2000 in
 hold-queue 2000 out
!
```



239645

QoS Policy Between Medium Campus and Main Campus Location

The medium campus location uses 4500 as WAN device, which uses 4500-E supervisor. The physical link speed is 100Mbps and the actual SLA is also 100Mbps. Therefore, a single-layer QoS policy meets the requirement.

4. Define the class-maps.

```
class-map match-all REALTIME
 match ip dscp cs4  af41  cs5  ef
class-map match-all CRITICAL_DATA
 match ip dscp af11 cs2  af21  cs3  af31 cs6
class-map match-all BEST_EFFORT
 match ip dscp default
class-map match-all SCAVENGER
 match ip dscp cs1
```

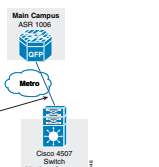
239646

5. Define the policy-maps.

```
policy-map RMC_POLICY
 class REALTIME
  priority
  police cir 33000000
   conform-action transmit
   exceed-action drop
  set cos 5
 class CRITICAL_DATA
  set cos 3
   bandwidth percent 36
 class SCAVENGER
   bandwidth percent 5
  set cos 0
 class BEST_EFFORT
  set cos 2
   bandwidth percent 25
!
```

285947

6. Apply the defined class and policy maps to the interface.




```
interface GigabitEthernet4/1
 description link connected to  cr13-6500-pe2 gi3/2
switchport trunk native vlan 802
switchport trunk allowed vlan 102
switchport mode trunk
logging event link-status
load-interval 30
carrier-delay msec 0
no cdp enable
spanning-tree portfast trunk
spanning-tree guard root
service-policy output RMC_POLICY
!
```

QoS Policy Implementation Between Remote Small Campus and Main Campus Location

The following section describes the QoS policy implementation between the remote small campus location and main campus. The physical link speed is T3, which is 45Mbps, but the SLA is 20 Mbps. Therefore, a hierarchical two-layer QoS policy is implemented. The parent policy shapes the link speed to 20Mbps and the child policy would queue and allocate the bandwidth within the 20Mbps.

1. Define the class-maps.

```
class-map match-all REALTIME
 match ip dscp cs4  af41  cs5  ef
class-map match-all CRITICAL_DATA
 match ip dscp af11  af21  cs3  af31 cs6
class-map match-all BEST_EFFORT
 match ip dscp default
class-map match-all SCAVENGER
 match ip dscp cs2
```

285949

2. Define the child policy map.

```
policy-map RSC_POLICY
 class REALTIME
   priority percent 33
 class CRITICAL_DATA
   bandwidth remaining percent 40
 class SCAVENGER
   bandwidth remaining percent 25
 class BEST_EFFORT
   bandwidth remaining percent 35
```

232650

3. Define the parent policy map.

```
policy-map RSC_PARENT_POLICY
 class class-default
  shape average 20000000
  service-policy RSC_POLICY
```

232651

4. Apply the policy map to interface.


```
interface Serial2/0
 dampening
 ip address 10.126.0.4 255.255.255.254
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp-key
 ip pim sparse-mode
 service-policy output RSC_PARENT_POLICY
 ip summary-address eigrp 100 10.124.0.0 255.255.0.0 5
 load-interval 30
 carrier-delay msec 0
 dsu bandwidth 44210
```

Redundancy

Redundancy must be factored into the WAN design for a number of reasons. Since the primary span across several service provider networks, it is likely that network will be subjected to different kinds of failures occurring all the time. One of the following failures

can occur over a period of time: route flaps, brownouts, fibers being cut, and device failures. The probability of these occurring over a short period of time is low, but the occurrence is highly likely over a long period of time. To meet these challenges, different kind of redundancy should be planned. The following are the some of the ways to support redundancy:

- NSF/SSO—For networks to obtain 99.9999% of availability, technologies such as NSF/SSO are needed. The NSF would route packets until route convergence is complete, where as SSO allows standby RP to take immediate control and maintain connectivity protocols.
- Service Software Upgrade (ISSU) allows software to be updated or modified while packet forwarding continues with minimal interruption.
- Ether channel load balancing—Enabling this feature provides link resiliency and load balancing of traffic. This feature is enabled on the WAN aggregation 2 device. Figure 17 shows where this feature is enabled.

Figure 17 Link Resiliency

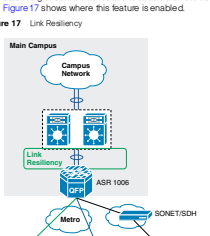


Table 3 shows the various WAN devices that are designed for resiliency.

Table 3 WAN Devices

Device	WAN transport	Resiliency feature
WAN aggregation 1	Private WAN/Internet	ISSU, IOS based redundancy
WAN aggregation 2	Metro	Redundant ESP, RP

This section discusses how to incorporate the resiliency principle in Cisco Community College reference design for the WAN design. To enable resiliency adds cost and complexity to the design. Therefore, resiliency has been added at certain places where it is absolutely critical to the network architecture rather than designing redundancy at every place of the network.

In the Cisco Community College reference design the redundancy is planned at both WAN aggregation router1, and WAN aggregation router 2 in the main campus location. As explained in the WAN aggregation platform selection for the main campus location discussion ASR routers have been selected at both WAN aggregation locations places. However, we have different models, at both WAN aggregation places. When the ASR router interfaces with the private WAN, Internet networks the ASR 1004 with IOS-based redundancy has been chosen. Similarly, for the ASR router that interfaces with Metro connections, the ASR 1006 with dual RP, and dual ESP to provide for hardware-based redundancy has been chosen. Both of these models support In Service Software Upgrade (ISSU) capabilities to allow a user to upgrade Cisco IOS XE Software while the system remains in service. To obtain more information on ASR resiliency capabilities, see the ASR page at following URL: http://www.cisco.com/go/asr1000

Implementing IOS-based Redundancy at WAN Aggregation Router 1

They key requirement for implementing software-based redundancy on the ASR1004 is you must have 4 GB DRAM on ASR1004. The following are steps for implementing the IOS based redundancy:

1. Check the memory on ASR 1004 router.

```
CR11-ASR-IE#show version
Cisco IOS Software, IOS-XE Software (PPC_LINUX_IOSD-ADVENTERPRISE-M),
Version 12.2(33)XND3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Tue 02-Mar-10 09:51 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2010 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON


 CR11-ASR-IE uptime is 3 weeks, 6 days, 2 hours, 4 minutes
Uptime for this control processor is 3 weeks, 6 days, 2 hours, 6 minutes
System returned to ROM by SSO Switchover at 14:41:38 UTC Thu Mar 18 2010
```

```
System image file is
"bootflash:asr1000rp1-adventerprise.02.04.03.122-33.XND3.bin"
Last reload reason: redundancy force-switchover



cisco ASR1004 (RP1) processor with 736840K/6147K bytes of memory.
5 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
937983K bytes of eUSB flash at bootflash:.
39004543K bytes of SATA hard disk at harddisk:.
15641929K bytes of USB flash at usb1:.

Configuration register is 0x2102

CR11-ASR-IE#
```

2. Enable the redundancy:

```
redundancy
 mode sso
!
```

3. Verify that redundancy is enabled:

```
CR11-ASR-IE#show redun
CR11-ASR-IE#show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 3 weeks, 6 days, 2 hours, 11 minutes
Switchovers system experienced = 3
              Standby failures = 0
        Last switchover reason = active unit removed

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 7
        Current Software state = ACTIVE
       Uptime in current state = 3 weeks, 6 days, 2 hours, 0 minutes
                 Image Version = Cisco IOS Software, IOS-XE Software
(PPC_LINUX_IOSD-ADVENTERPRISE-M), Version 12.2(33)XND3, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Tue 02-Mar-10 09:51 by mcpre
                           BOOT =
bootflash:asr1000rp1-adventerprise.02.04.03.122-33.XND3.bin,1;
                      CONFIG_FILE =
        Configuration register = 0x2102

Peer Processor Information :
----------------------------
              Standby Location = slot 6
        Current Software state = STANDBY HOT
       Uptime in current state = 3 weeks, 6 days, 1 hour, 59 minutes
                 Image Version = Cisco IOS Software, IOS-XE Software
(PPC_LINUX_IOSD-ADVENTERPRISE-M), Version 12.2(33)XND3, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Tue 02-Mar-10 09:51 by mcpre
                           BOOT =
bootflash:asr1000rp1-adventerprise.02.04.03.122-33.XND3.bin,1;
                      CONFIG_FILE =
        Configuration register = 0x2102



CR11-ASR-IE#
```

Implementation of Hardware-based Redundancy at WAN Aggregation Router 2

As explained in the design considerations documents, the WAN aggregation router 2 has redundant RPs and redundant ESPs. Therefore, with this configuration, we can achieve non-stop forwarding of data even when there failures with either ESP or RPs. The following steps are needed to enable hardware redundancy on WAN aggregation router 2:

1. Configuration of SSO redundancy:

```
redundancy
 mode sso
```

2. Verify the redundancy information:

```
cr11-asr-we#show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 3 weeks, 6 days, 3 hours, 32 minutes
Switchovers system experienced = 4
              Standby failures = 0
```

```
        Last switchover reason = active unit removed

                  Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
       Maintenance Mode = Disabled
                 Communications = Up


Current Processor Information :
-------------------------------
                 Active Location = slot 6
          Current Software state = ACTIVE
         Uptime in current state = 2 weeks, 1 day, 19 hours, 3 minutes
                   Image Version = Cisco IOS Software, IOS-XE Software
(PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Version 12.2(33)XND2, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 04-Nov-09 18:53 by mcpre
                        BOOT =
                   CONFIG_FILE =
          Configuration register = 0x2102

Peer Processor Information :
----------------------------
                 Standby Location = slot 7
          Current Software state = STANDBY HOT
         Uptime in current state = 2 weeks, 1 day, 18 hours, 52 minutes
                   Image Version = Cisco IOS Software, IOS-XE Software
(PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Version 12.2(33)XND2, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 04-Nov-09 18:53 by mcpre
                        BOOT =
                   CONFIG_FILE =
          Configuration register = 0x2102


cr11-asr-we#
```

Implementation of Link Resiliency Between the WAN Aggregation Router 2 and VSS Core

The following are implementation steps to deploy link resiliency:

1. Configure the ether channel between the ASR1006 and the VSS core.

```
interface GigabitEthernet0/2/3
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 negotiation auto
 cdp enable
 service-policy output WAN_Upstream
 channel-group 1 mode active
 hold-queue 2000 in
 hold-queue 2000 out
!
interface GigabitEthernet0/2/4
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 negotiation auto
 cdp enable
 service-policy output WAN_Upstream
 channel-group 1 mode active
 hold-queue 2000 in
 hold-queue 2000 out
!
Step 2) Configure the port-channel interface
interface Port-channel1
 ip address 10.125.0.23 255.255.255.254
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp-key
 ip pim sparse-mode
 ip summary-address eigrp 100 10.126.0.0 255.255.0.0 5
 logging event link-status
 load-interval 30
 carrier-delay msec 0
 negotiation auto
!
```

Multicast

The main design considerations for multicast are as follows:

- The number of groups supported by the WAN edge device. This is scalability factor of the WAN edge device. The platform chosen must support the number of required groups.
- The placement of the RP—There are couple of options available with RP placement, which include Anycast with Static, Anycast with Auto-RP, or Anycast with BSR.
- Multicast protocols—PIM-Sparse mode, IGMP

- QoS policy must be configured for multicast traffic, so that this traffic does not affect the unicast traffic.

In the Community College Reference design, we are assuming that multicast traffic would be present only within the campus, and not between the community colleges. Hence the multicast design looks at only between the main campus, and remote small campus locations. The implementation section in the document shows how to enable multicast on the WAN device only. Therefore, to obtain more information about multicast design for campus, refer to *Community College LAN Deployment Guide*.

Multicast Configuration on WAN Aggregation Router 2

This section shows how to enable multicast routing, and what interfaces to be enabled with PIM-Sparse mode on the WAN aggregation router2 that connects to different remote campus sites.

1. Enable multicast routing.

```
ip multicast-routing distributed
```

2. Enable PIM-Spare mode on the following WAN interfaces.
   - Port-channel—Connects to the VSS core
   - Gi0/2/0—Connects to remote large campus site
   - Gi0/2/1—Connects to remote medium campus site
   - S0/3/0—Connects to remote small campus site

```
interface Port-channel1
 ip address 10.125.0.23 255.255.255.254
 ip pim sparse-mode
  negotiation auto
!
interface GigabitEthernet0/2/0
 description Connected to cr11-3750ME-RLC
 ip address 10.126.0.1 255.255.255.254
 ip pim sparse-mode
 logging event link-status
 load-interval 30
 negotiation auto
!
interface GigabitEthernet0/2/1
 description Connected to cr11-4507-RMC
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 negotiation auto
 cdp enable
 hold-queue 2000 in
 hold-queue 2000 out
!
interface GigabitEthernet0/2/1.102
 encapsulation dot1Q 102
 ip address 10.126.0.3 255.255.255.254
 ip pim sparse-mode
 !
!
interface Serial0/3/0
 dampening
 ip address 10.126.0.5 255.255.255.254
 ip pim sparse-mode
 load-interval 30
 carrier-delay msec 0
 dsu bandwidth 44210
 framing c-bit
 cablelength 10
!
Step 3) Configure the RP location
ip pim rp-address 10.100.100.100
```

Configuration of Multicast on Remote Large campus

This section discusses how to implement multicast on remote large campus site. The following are implementation steps:

1. Enable multicast routing.

```
ip multicast-routing distributed
```

2. Enable pim sparse mode on the WAN interface that connects to main campus site.

```
interface GigabitEthernet1/1/1
 description Connected to cr11-ASR-WE
 no switchport
 dampening
 ip address 10.126.0.0 255.255.255.254
 ip pim sparse-mode
 hold-queue 2000 in
 hold-queue 2000 out
!
```

Configuration of Multicast on Remote Medium Campus

This section discusses on how to implement multicast on remote medium campus site.

1. Enable multicast routing.

```
ip multicast-routing
```

2. Enable PIM Spare mode on the WAN interface:

```
interface Vlan102
 description Connected to cr11-ASR-WE
 dampening
 ip address 10.126.0.2 255.255.255.254
 ip pim sparse-mode
 load-interval 30
 carrier-delay msec 0
```

Configuration of Multicast on Remote Small Campus Site

This section discusses on how to implement multicast on remote small campus site.

1. Enable multicast routing.

```
ip multicast-routing
```

2. Enable PIM Spare mode on the WAN interface:

```
interface Serial2/0
 dampening
 ip address 10.126.0.4 255.255.255.254
 ip pim sparse-mode
 load-interval 30
 carrier-delay msec 0
 dsu bandwidth 44210
```

3. Configure the RP location:

```
ip pim rp-address 10.100.100.100 Allowed_MCAST_Groups override
```

4. Configure the Multicast security:

```
ip pim spt-threshold infinity
ip pim accept-register list PERMIT-SOURCES
!
ip access-list standard Allowed_MCAST_Groups
 permit 224.0.1.39
 permit 224.0.1.40
 permit 239.192.0.0 0.0.255.255
 deny   any
ip access-list standard Deny_PIM_DM_Fallback
 deny   224.0.1.39
 deny   224.0.1.40
 permit any
!
ip access-list extended PERMIT-SOURCES
 permit ip 10.125.31.0 0.0.0.255 239.192.0.0 0.0.255.255
 deny   ip any any
!
```

Summary

Designing the WAN network aspects for the Cisco Community College reference design interconnects the various LAN locations as well as lays the foundation to provide safety and security, operational efficiencies, virtual learning environments, and secure classrooms.

This chapter reviewed the WAN design models recommended by Cisco and where to apply these models within the various locations within a community college network. Key WAN design principles such as WAN aggregation platform selection, QoS, multicast and redundancy best practices were discussed for the entire community college design. Designing the WAN network of a community college using these recommendations and best practices will establish a network that is resilient in case of failure, scalable for future grown, simplified to deploy and manage and cost efficient to meet the budget needs of a community college.